International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 8 Issue 10 October - 2024, Pages: 83-106

Smart Building Technologies: A Comprehensive Review of IoT Applications in the Built Environment

Muhammad Abubakar[1*], Ibrahim Halima D[2], Muhammad Aliyu[3], Shodeke Sunday[4]

[1,2] Nigerian Building Road Research Institute, Department of Building Research, Abuja, Nigeria
[3]Nigerian Building and Road Research Institute, Department of Science Laboratory Technology, North West Zonal Office, Kano State, Nigeria.
[4]Federal Polytechnic, Department of Civil Engineering, Ilaro Ogun state, Nigeria.

Corresponding author email: *olabode4angel@gmail.com*

Abstract: *The rapid advancement of Internet of Things (IoT) technologies has profoundly transformed the built environment, leading to the emergence of smart buildings that prioritize energy efficiency, occupant comfort, and sustainability. This comprehensive review explores the diverse applications of IoT within smart building technologies, focusing on their impact on building management systems, indoor environmental quality (IEQ), and energy consumption. The study synthesizes current research and case studies to illustrate how IoT-enabled sensors, data analytics, and automation systems are utilized to optimize heating, ventilation, and air conditioning (HVAC) systems, monitor indoor air quality, and enhance occupant well-being. Also, the integration of IoT with other technologies such as artificial intelligence (AI) and big data, which further enhances the intelligence and responsiveness of building systems. While the benefits of IoT in smart buildings are substantial, the paper as well addresses the challenges associated with cybersecurity, data privacy, and the interoperability of various devices. By providing a holistic overview of IoT applications in smart buildings, the review offers valuable insights for architects, engineers, and policymakers aiming to design and manage buildings that meet the demands of modern occupants while reducing environmental impact. The findings highlight the potential of IoT to revolutionize the built environment, paving the way for more sustainable and intelligent building solutions.*

Keywords: Smart Building Technologies, Internet of Things (IoT), Built Environment, Building Management Systems, Indoor Environmental Quality (IEQ).

1. INTRODUCTION

The rapid pace of urbanization, coupled with the increasing global demand for energy-efficient, sustainable, and user-friendly environments, has significantly accelerated the development and adoption of smart building technologies. As cities continue to expand and populations grow, the need for buildings that can efficiently manage resources, reduce environmental impact, and enhance the quality of life for occupants has become more pressing. Smart building technologies, powered by the Internet of Things (IoT), offer a solution to these challenges by creating interconnected systems capable of monitoring, analyzing, and controlling various building functions in real-time [1].

IoT enables the seamless integration of a wide array of sensors, devices, and software platforms, transforming traditional buildings into intelligent, responsive environments.

These smart environments can autonomously adjust lighting, heating, ventilation, and air conditioning (HVAC) systems based on occupancy patterns, weather conditions, and energy consumption data. This not only improves energy efficiency but also enhances the comfort and safety of building occupants [2].

Additionally, IoT facilitates the integration of renewable energy sources, smart grids, and energy storage systems, contributing to the sustainability of buildings and supporting broader environmental goals [3].

The application of IoT in building security systems was emphasized by Xu *et al*. (2023) in one of the early researches in this field. The authors gave an example of how an inexpensive, simple-to-install home security system might enable family members to keep an eye on the security and environmental conditions in their house in real time using WeChat.

[4]. Building on this study, Alkhudaydi *et al.* (2023) looked into how AI and IoT may be combined to create smarter security systems. Their study shown that balancing algorithms such as SMOTE, when paired with machine and deep learning approaches, may successfully detect intrusions into Internet of Things networks with accuracy rates of 98.19% and 98.50%, respectively. [5]. However, while the study demonstrated AI's potential in data analysis, it did not fully explore AI's ability to autonomously make security decisions in real-time, leaving a gap in the research on fully autonomous AI-IoT security solutions.

Tariq *et al*. (2023) conducted a comprehensive review of IoT security challenges, focusing on the vulnerabilities that arise from the vast number of interconnected devices. Their work identified significant cybersecurity risks, such as hacking, data breaches, and unauthorized access, that could compromise IoT-based security systems. While the study focused on the security risks associated with IoT, it did not

explore how AI could be used to mitigate these risks. This gap leaves room for further investigation into the role of AI in enhancing the cybersecurity of IoT networks, particularly through predictive threat detection and automated response mechanisms [6].

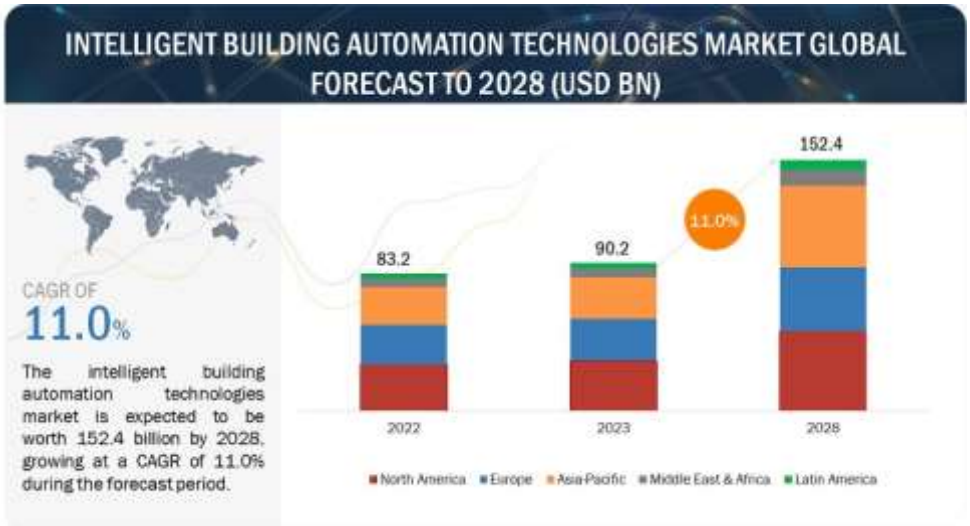
In a more recent study, Alkhudaydi *et al*. (2023) specifically examined the integration of AI and IoT in building security systems, focusing on the advancements in predictive analytics and automated decision-making. They argued that AI's ability to process and learn from data collected by IoT devices was a game changer for security management, enabling systems to predict and preempt security threats before they occur. Their study provided a more in-depth exploration of AI's role in real-time decision-making for security responses, setting the stage for further research on the operational effectiveness of AI-IoT integration. However, they also noted challenges in ensuring the interoperability of different AI and IoT platforms, as well as the need for enhanced cybersecurity to protect the sensitive data processed by these systems [5].

Another significant contribution was made by Balti *et al*. (2023**)**, who examined the use of AI-driven behavioral analytics in IoT-based smart building environments. Their research explored how AI could track and analyze occupant behavior to identify abnormal activities that might indicate security risks. This work represented a notable advancement in the field, as it highlighted AI's ability to go beyond traditional rule-based security systems and adaptively learn from behavioral patterns [7]. Nevertheless, the study was primarily theoretical and lacked extensive real-world applications or case studies to validate these findings. While these studies collectively illustrate the significant advancements in AI and IoT for security management, several gaps remain in the literature. Many works focus on the individual capabilities of IoT or AI but fall short of providing a comprehensive understanding of how the two can be fully integrated for real-time, autonomous security decision-making. Additionally, there is limited research on the challenges posed by cybersecurity threats to AI-IoT systems, and how AI can be used to mitigate these risks. Furthermore, ethical concerns surrounding privacy, surveillance, and the potential biases in AI-driven security decisions have yet to be thoroughly explored.

Similarly, issues such as data privacy, cybersecurity, and system interoperability remain largely unresolved, especially in retrofitting older buildings. Furthermore, the high costs associated with the adoption of IoT technologies present additional challenges for widespread implementation [8]. These gaps highlight the need for a comprehensive review that not only outlines the state-of-the-art IoT applications but also critically examines the challenges and opportunities for further innovation.

This review seeks to fill this research gap by providing an in-depth analysis of IoT applications in the built environment, exploring the technological, economic, and regulatory challenges. In addition, it will examine emerging trends such as artificial intelligence (AI), machine learning, and edge computing that promise to enhance the future capabilities of smart building systems [9]. Through this examination, the paper aims to contribute to the ongoing discourse on the future of sustainable urban development.

The review will address the challenges faced in implementing IoT technologies in the built environment, including issues related to data privacy, cybersecurity, interoperability, and the high costs associated with retrofitting existing structures. Despite these challenges, the potential benefits of IoT integration are substantial, offering opportunities for significant improvements in building performance and sustainability. The paper will also explore emerging trends in IoT-enabled smart buildings, such as the integration of artificial intelligence (AI), machine learning, and edge computing, which are poised to further enhance the capabilities of smart building systems.



Figures 1. An infographic showing the growth of smart building technologies and the projected market size for IoT in the built environment [10].

2. IOT applications in smart buildings

2.1 Energy Management

Energy management is a fundamental aspect of smart building technologies, increasingly driven by the global imperative to reduce energy consumption and mitigate carbon emissions. The growing awareness of climate change and the rising costs of energy have led to the development and integration of advanced IoT-enabled systems within buildings. These systems, which include smart meters, HVAC controls, and intelligent lighting, play a pivotal role in optimizing energy use by enabling real-time monitoring, analysis, and dynamic adjustment of building operations [11].

Smart meters, for instance, are essential components of modern energy management systems. They provide detailed, real-time insights into energy consumption patterns at various levels, from individual devices to entire buildings. This granular data allows building managers to identify inefficiencies, track energy usage trends, and make informed decisions that enhance energy efficiency. The continuous monitoring facilitated by smart meters also enables the implementation of demand response strategies, where energy consumption can be adjusted during peak periods to avoid overloading the grid and incurring higher energy costs [12].

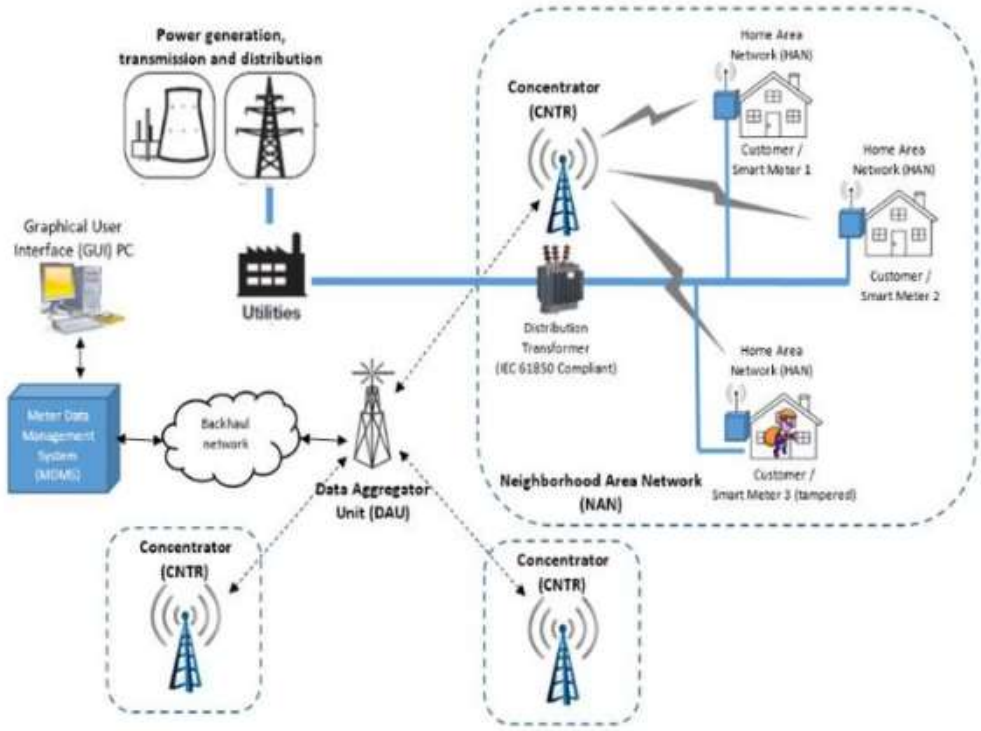


Figure 2. Schematic of a smart meter system, illustrating real-time data collection, analysis, and energy optimization processes [13].

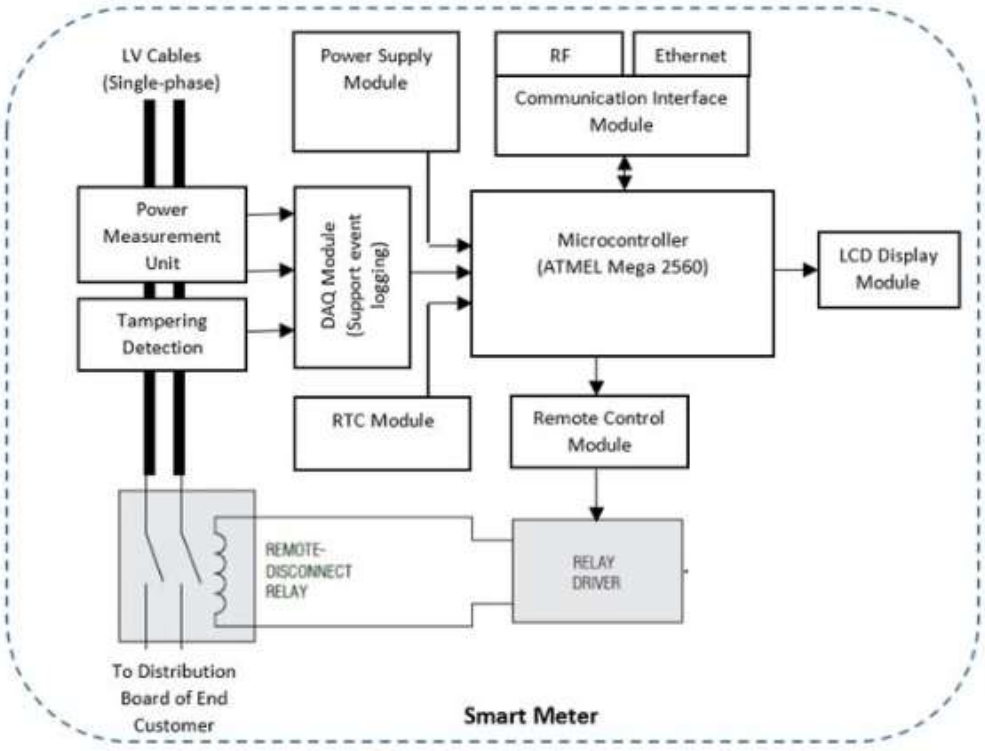


Figure 3. The hardware design of smart meter unit [14].

HVAC systems, traditionally one of the most energy-intensive components of a building, have also been significantly improved through IoT integration. IoT-enabled HVAC controls allow for precise adjustments based on a combination of factors, including occupancy patterns, external weather conditions, and indoor air quality. Smart thermostats, a key component of these systems, can autonomously regulate heating and cooling based on real-time data, ensuring that energy is used only when and where it is needed. This level of control not only reduces energy waste but also enhances occupant comfort by maintaining consistent indoor conditions [15].

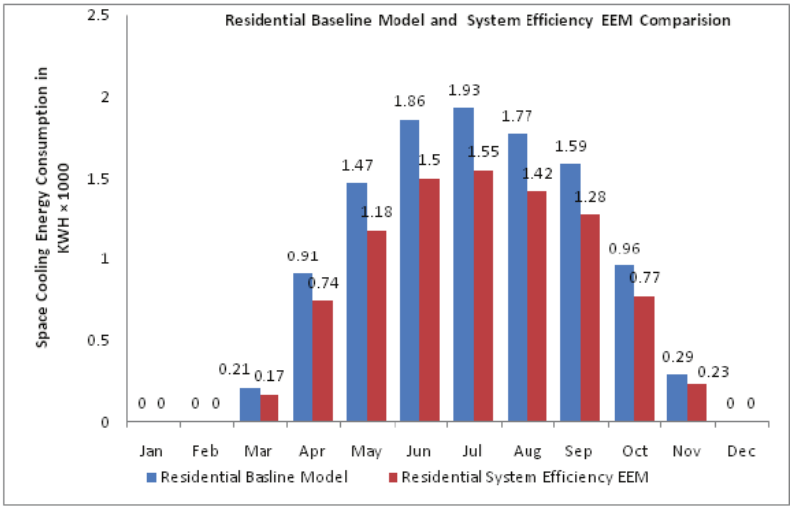


Figure 4. Comparison of Residential Baseline and Energy efficient Models [16].

Table 1. Comparison of Energy Consumption in Buildings Using Conventional HVAC Systems vs. IoT-Enabled Smart HVAC Controls

HVAC System Type	Average Energy Consumption (kWh/m²/year)	Energy Savings (%)	Operational Efficiency	Reference
Conventional HVAC Systems	40	Baseline (0%)	Moderate: Limited by fixed settings and lack of real-time adaptability	[17]
IoT-Enabled Smart HVAC Controls	21.81- 44.36	30–40%	High: Adaptive to real-time data, optimizing energy use based on occupancy and environmental conditions	[18]

Moreover, IoT-enabled lighting systems contribute significantly to energy management by optimizing the use of artificial lighting. These systems are equipped with sensors that detect occupancy and ambient light levels, allowing them to adjust lighting intensity automatically. For example, lights in unoccupied rooms can be dimmed or switched off entirely, and lighting can be reduced during periods of high natural light availability. This not only lowers energy consumption but also extends the lifespan of lighting fixtures, resulting in additional cost savings over time [19].

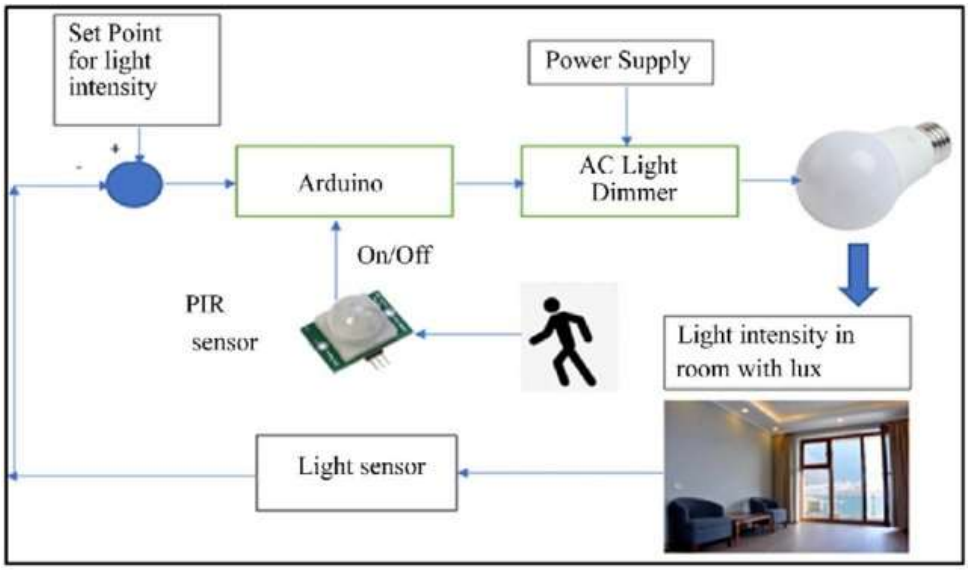


Figure 5. Diagram depicting the operation of a smart lighting system, highlighting the interaction between occupancy sensors and lighting controls [20].

In addition to optimizing individual systems, IoT facilitates the integration of renewable energy sources, such as solar panels, into building energy grids. This integration enables the efficient management of energy supply and demand, further enhancing sustainability [21].

2.2 Enhanced Building Security through IoT Integration

The integration of Internet of Things (IoT) technologies into building security systems has revolutionized traditional security practices by introducing advanced surveillance, access control, and threat detection capabilities. These innovations, driven by IoT-enabled devices such as high-resolution cameras, motion sensors, and smart locks, have significantly improved the ability to monitor and respond to security incidents in real-time.

2.2.1 Advanced Surveillance Systems

IoT-enabled surveillance systems are a cornerstone of modern building security. High-resolution cameras, equipped with features like night vision and wide-angle lenses, provide continuous monitoring and detailed visual data. These cameras are often connected to a centralized network,

allowing for real-time video streaming and remote access by security personnel. The deployment of these cameras in strategic locations across a building not only enhances visibility but also enables the integration of AI and machine learning algorithms, which can analyze video feeds for unusual patterns or behaviors. For instance, AI can automatically detect and flag suspicious activities, such as unauthorized access attempts or loitering, and trigger alerts for immediate action [22].

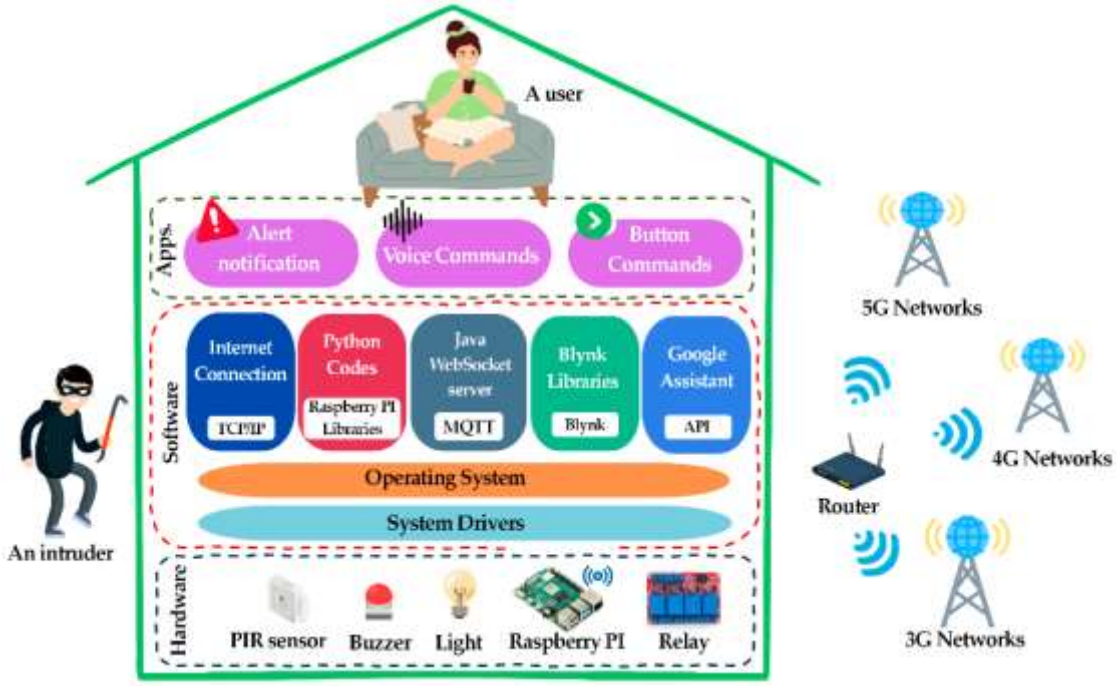


Figure 6. Diagram illustrating the components of an IoT-enabled surveillance system, including high-resolution cameras, AI analytics, and data processing units [23].

2.2.2 Smart Access Control Mechanisms

Access control is another critical area where IoT technologies have made substantial improvements. Traditional key-based systems are being replaced by smart locks and biometric access controls, which offer enhanced security and convenience. IoT-enabled smart locks can be operated remotely, allowing building managers to grant or revoke access in real-time through a mobile app or centralized control system. These systems can also be integrated with facial recognition technology, further strengthening security by ensuring that only authorized individuals can enter restricted areas. The implementation of such access control mechanisms not only improves security but also simplifies the management of building access, particularly in large or multi-tenant buildings [24].

Table 2. Comparative analysis of traditional access control systems versus IoT-enabled smart locks, highlighting differences in security features, convenience, and cost [19].

Topic	Traditional internet	IoT
Who creates contents?	Human	Machine
How is the content combined?	Using explicitly defined links	Through explicitly defined operations
What is the value?	Answered questions	Actions and timely information
What was done so far?	Both content creation (HTML) and content consumption (search engine)	Mainly content creation
Type of connections	Point to point and multipoint	Only multipoint
Digital Data	Readily available	Does not generate unless augmented or manipulated
Technology concept based on	Both physical-fist and digital- fist	Physical-fist

2.3 Proactive Threat Detection and Response

IoT technologies excel in proactive threat detection, an area where traditional security systems often fall short. Motion sensors, environmental sensors, and other IoT devices continuously monitor the building environment for anomalies. When these devices are coupled with AI, the system can analyze data in real-time to identify potential security threats, such as unauthorized entry, unusual movements, or environmental hazards like fire or gas leaks. AI-driven predictive analytics can forecast potential security breaches by identifying patterns that precede such incidents, allowing for preemptive action to be taken, such as locking down areas or alerting security personnel [25].

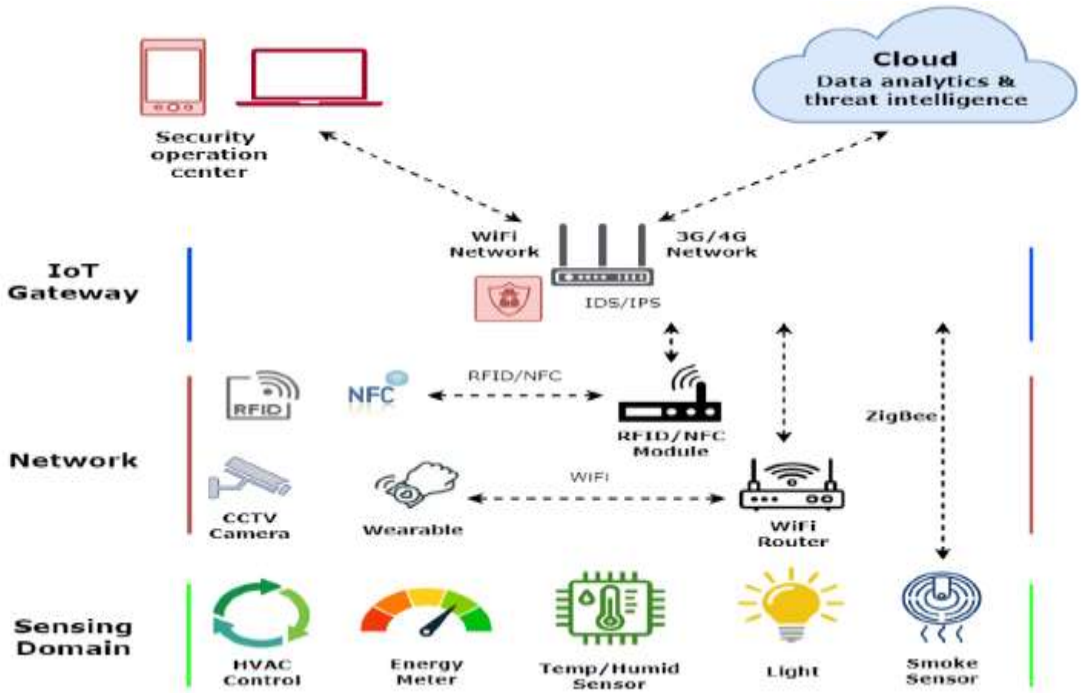


Figure 7. Flowchart showing the process of threat detection and automated response in an IoT-based security system, from sensor data collection to action execution [26].

2.4 Advanced Security Management through AI and IoT Integration

The integration of Artificial Intelligence (AI) and Machine Learning (ML) with Internet of Things (IoT) security systems has brought a new level of sophistication to building security management. This convergence enables predictive analytics, which leverages the vast amounts of data collected by IoT devices to anticipate and mitigate security threats before they materialize. By analyzing patterns and behaviors detected by sensors, AI can make real-time decisions that significantly enhance the effectiveness of security systems [27].

2.4.1 Predictive Analytics in Security

Predictive analytics is one of the most powerful tools enabled by the integration of AI with IoT. Through continuous data collection from various IoT devices, such as motion sensors, cameras, and access controls, AI systems can identify patterns that precede potential security breaches. For example, an AI-driven system might analyze movement patterns within a building and recognize anomalies, such as unauthorized access to restricted areas or unusual activity during off-hours. These systems use algorithms that learn from historical data to improve their predictive accuracy over time [28].

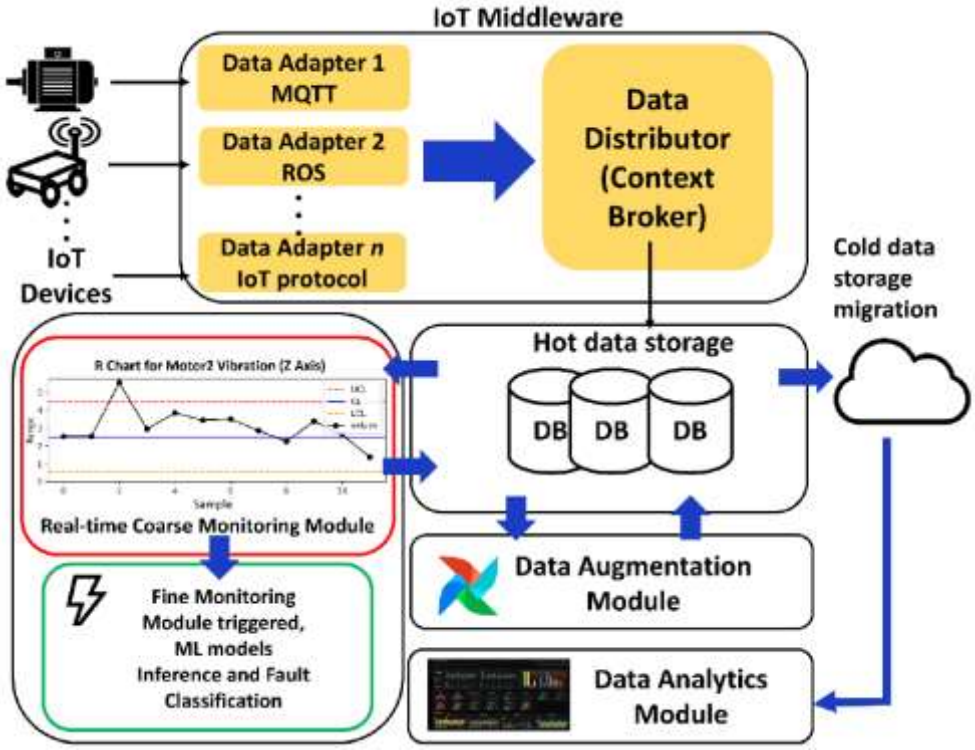


Figure 8. Illustration of a predictive analytics workflow in an IoT-enabled security system, showing data collection, pattern recognition, and automated response [29].

2.4.2 Automated Security Protocols

Once a potential threat is identified through predictive analytics, the AI system can trigger automated security protocols. This process reduces the need for human intervention and allows for a faster, more accurate response to security threats. if an unusual pattern of movement is detected, the system might automatically lock down certain areas of the building, activate alarms, or send real-time notifications to security personnel. This capability is particularly valuable in large or complex buildings where manual monitoring and response might be slow or insufficient [30].

Table 3. Comparison of Response Times and Accuracy Between Traditional Security Systems and AI-Enabled IoT Security Systems

Security System Type	Response Time	Accuracy	Operational Characteristics
Traditional Security Systems	Moderate to Slow	Moderate	Relies on manual monitoring and pre-set alerts; limited ability to analyze and adapt in real-time.
AI-Enabled IoT Security Systems	Fast to Instantaneous	High	Utilizes real-time data processing and machine learning algorithms for adaptive threat detection and response.

This table compares traditional security systems with AI-enabled IoT security systems in terms of response time, accuracy, and operational characteristics.

Traditional security systems are characterized by moderate to slow response times due to their reliance on manual monitoring and predefined alert mechanisms. These systems typically require human intervention to analyze security footage or data, which can delay responses. Additionally, their accuracy is moderate, as they often depend on simple sensor inputs and lack advanced analytical capabilities, leading to potential false positives or missed threats [31].

AI-enabled IoT security systems offer significant improvements, with response times ranging from fast to instantaneous. These systems leverage real-time data processing, machine learning algorithms, and advanced sensors to detect and respond to security threats more effectively. The integration of AI enhances the accuracy of threat detection by continuously learning and adapting to new

patterns, reducing the likelihood of false alarms and improving overall security outcomes [32].

This comparison highlights the advancements brought by AI and IoT technologies in security systems, emphasizing the benefits of faster response times and higher accuracy in protecting assets and occupants.

2.4.3 Real-Time Threat Response

The ability to respond to threats in real-time is a key advantage of integrating AI with IoT in security systems. Traditional security measures often rely on post-incident analysis, where security staff review footage or logs after a breach has occurred. In contrast, AI-enabled systems can analyze data as it is collected, allowing for immediate responses to potential threats. This shift from reactive to proactive security management significantly enhances the safety and security of the building environment, as threats can be neutralized before they escalate [33].

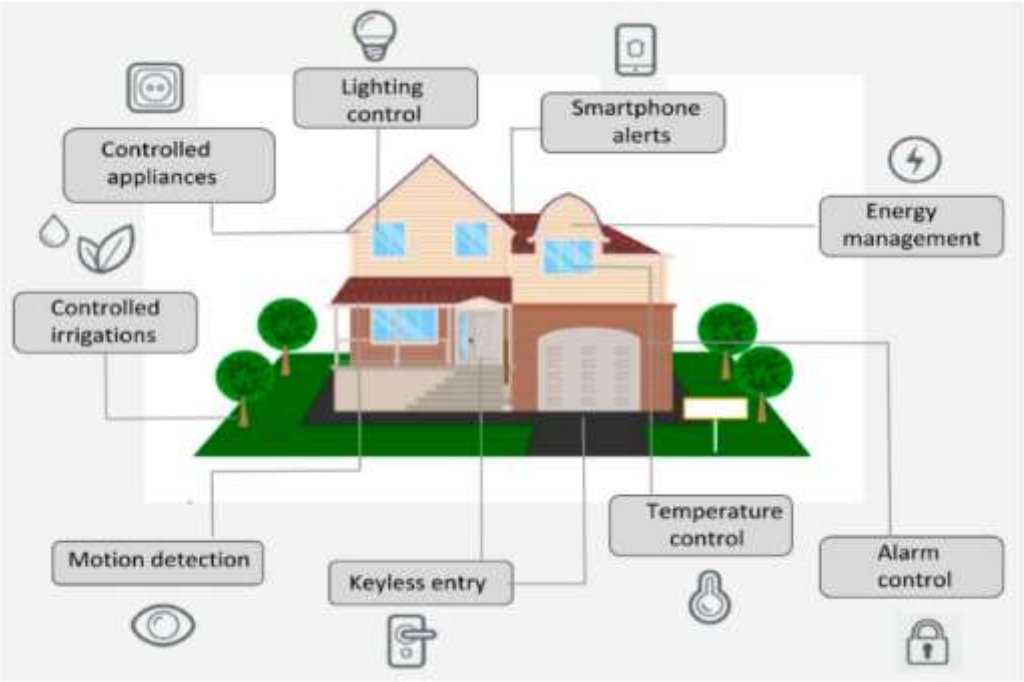


Figure 9. Diagram depicting a real-time threat detection and response system, with IoT sensors feeding data to an AI engine that processes information and triggers automated actions [34].

2.4.4 Enhanced Accuracy and Reduced Human Error

The use of AI and ML in IoT security systems also reduces the likelihood of human error. Traditional security operations often involve manual monitoring and decision-making, which can be prone to mistakes, especially in high-pressure situations.

AI systems, however, process large datasets with precision, identifying subtle patterns that human operators might overlook. As these systems continue to learn from new data, their accuracy in predicting and responding to security threats improves, providing a higher level of protection for building occupants and assets [35].

Table 4. Summary of the Advantages of AI-Enabled IoT Security Systems Over Traditional Methods

Advantage	AI-Enabled IoT Security Systems	Traditional Security Methods
Accuracy	High precision in threat detection and anomaly detection through continuous learning and pattern recognition.	Often relies on predefined rules and manual processes, leading to potential human errors and false positives.
Response Time	Real-time monitoring and instant response capabilities, minimizing damage and enhancing protection.	Typically, slower, as it depends on manual intervention and predefined thresholds for alerts.
Scalability	Easily scalable across various devices and networks, adapting to growing infrastructure needs with minimal additional costs.	Limited scalability, requiring significant investments in hardware and labor for expansion.

Threat Adaptation	Dynamic adaptation to emerging threats through machine learning and AI algorithms.	Static approach with delayed updates, making it vulnerable to new and evolving threats.
Data Processing	Capable of processing large volumes of data from multiple sources simultaneously, improving overall system efficiency.	Struggles with large data volumes, leading to potential delays in threat detection and response.

Table 5. Summary of Predictive Analytics Techniques Used in IoT-Based Security Systems

Technique	Description	Application in IoT-Based Security
Pattern Recognition	Involves identifying regularities and patterns within data streams, allowing the system to recognize normal behavior and detect deviations	Utilized to establish baseline behavior in IoT devices, enabling the detection of unusual activities that may indicate security breaches.
Anomaly Detection	Refers to the identification of outliers or deviations from established patterns, which could signal potential threats	Critical for real-time monitoring of IoT networks, facilitating the early detection of suspicious activities that may bypass traditional defenses.
Threat Forecasting	Employs machine learning algorithms to predict potential security threats based on historical data and trend analysis	Enhances proactive security measures by anticipating future threats, allowing preemptive actions to be taken to mitigate risks.

In this table, predictive analytics techniques such as pattern recognition, anomaly detection, and threat forecasting are highlighted as key components in enhancing the security of IoT-based systems. These techniques are instrumental in identifying potential threats and mitigating risks in real time, thus improving the overall security posture of IoT environments [36]; [37].

2.5 Access Control Mechanisms

Smart access control systems, a key application of IoT technology, enhance building security through advanced features like remote management and real-time monitoring of entry points. Smart locks and access control systems allow for keyless entry, remote unlocking, and real-time tracking of access events. These systems can be managed through mobile applications or centralized control panels, providing flexibility and increased security. Features such as temporary access codes and detailed access logs further enhance security by controlling and monitoring who enters and exits the building [38].

-

Table 6. Comparative Analysis of Traditional Access Control Systems Versus IoT-Enabled Smart Locks

Feature	Traditional Access Control Systems	IoT-Enabled Smart Locks
Remote Management	Typically requires physical presence for access control management and key distribution.	Allows remote management through mobile apps or web interfaces, enabling real-time control from any location.
Keyless Entry	Primarily relies on physical keys or access cards, with potential issues such as loss or duplication.	Facilitates keyless entry via digital credentials, biometrics, or mobile devices, reducing the risk of unauthorized access.
Access Logs	Limited or non-existent logging, often dependent on manual entry or basic electronic records.	Automatically generates detailed access logs with time stamps, enhancing security and auditability.

This table provides a comparative analysis of traditional access control systems versus IoT-enabled smart locks, emphasizing key features such as remote management, keyless entry, and access logs. Traditional systems generally lack the flexibility and advanced functionalities offered by IoT-enabled smart locks, which provide enhanced security and convenience through features like remote management and detailed access logs
[39]; [40].

2.6 Threat Detection Capabilities

IoT technologies significantly improve threat detection capabilities through the use of various sensors and data analytics. Motion sensors and environmental sensors (detecting smoke or gas leaks) can detect anomalies in real-time and trigger alerts. When integrated with AI, these sensors can analyze patterns and predict potential security threats before they materialize. For instance, an AI-driven system might use data from motion sensors to identify unusual

patterns that indicate a possible break-in or unauthorized movement, allowing for preemptive action [41].

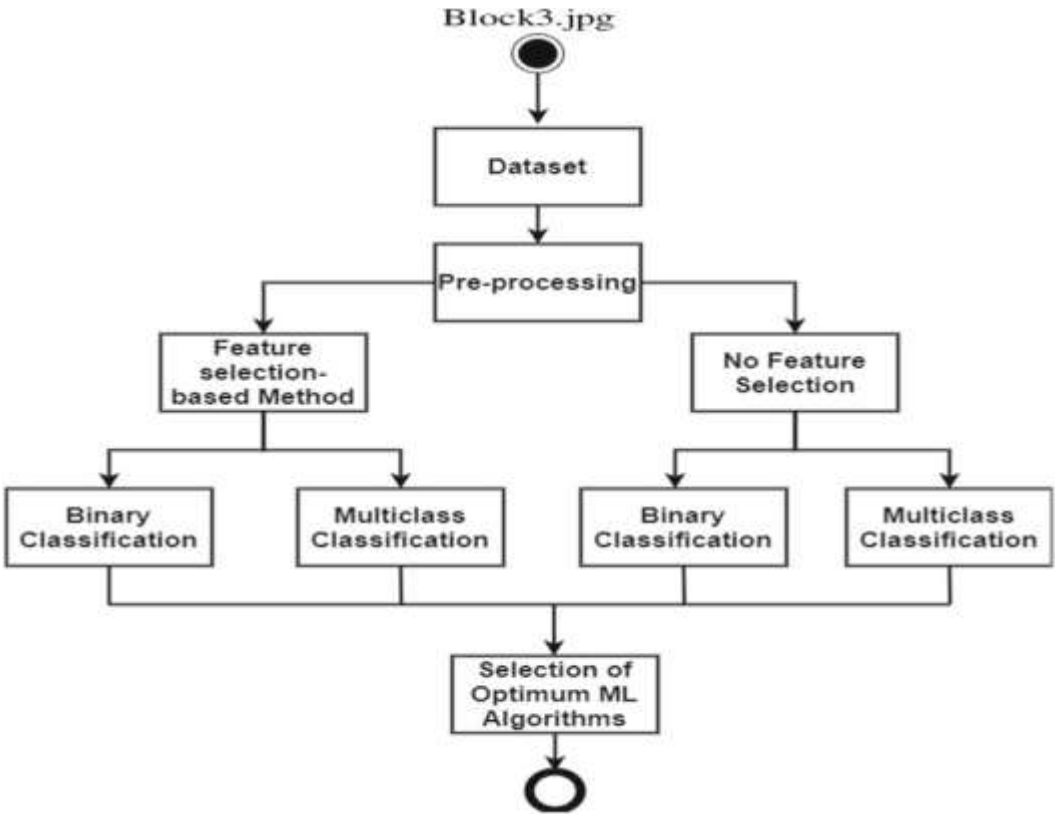


Figure 10. Flowchart showing the process of threat detection and automated response in an IoT-based security system, from sensor data collection to action execution [42].

2.7 Indoor Environmental Quality

Maintaining optimal indoor environmental quality (IEQ) is crucial for ensuring occupant health, comfort, and productivity within buildings.

The advent of Internet of Things (IoT) technologies has significantly enhanced the capability to monitor and control various environmental parameters such as temperature, humidity, air quality, and lighting levels. By leveraging IoT sensors, buildings can continuously collect real-time data, which is then utilized to automatically adjust building systems to maintain ideal conditions [43].

2.7.1 Temperature and Humidity Control

Temperature and humidity are critical factors influencing indoor comfort and health. IoT sensors embedded in smart building systems continuously monitor these parameters and relay the data to central control systems. Smart HVAC systems, which integrate with these sensors, can adjust heating, cooling, and ventilation based on real-time data. For instance, if the temperature or humidity levels deviate from predefined comfort ranges, the system can automatically regulate the HVAC operations to bring conditions back to optimal levels. This not only enhances occupant comfort but also reduces energy consumption by preventing overuse of HVAC systems [44].

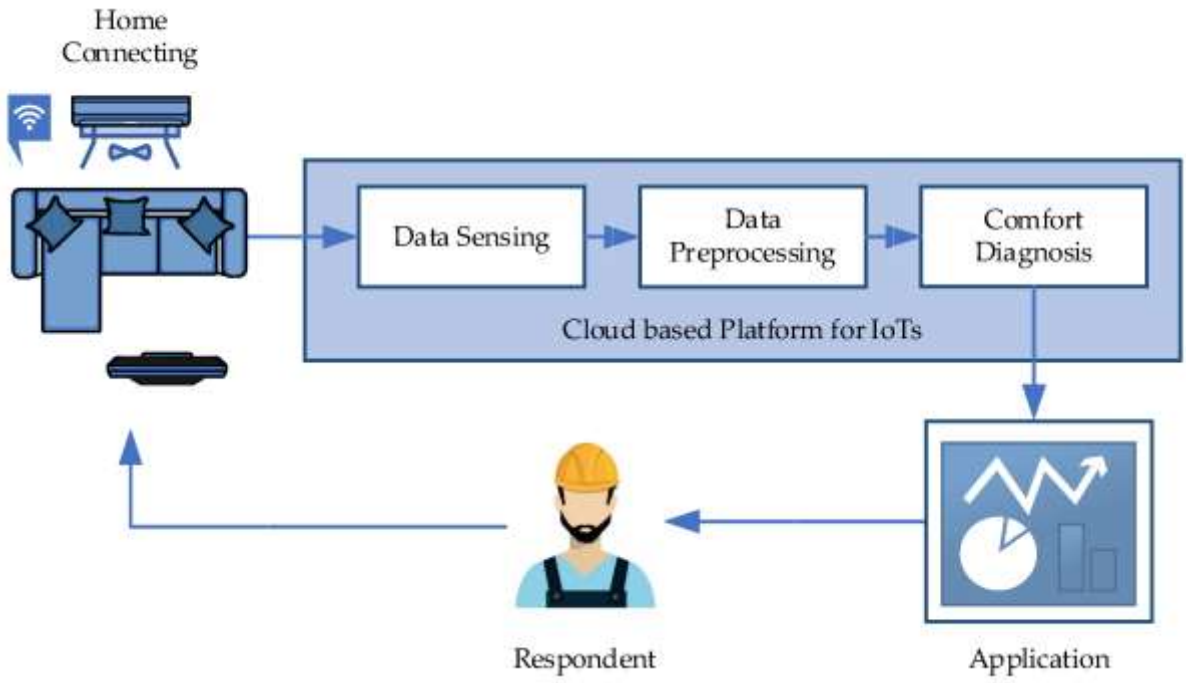


Figure 11. Diagram of an IoT-enabled HVAC system illustrating the interaction between temperature and humidity sensors, control systems, and HVAC units. [45].

2.7.2 Air Quality Management

Indoor air quality (IAQ) is another critical component of IEQ, as poor air quality can lead to health issues such as respiratory problems and allergies. IoT sensors that measure various air quality indicators—such as particulate matter (PM), carbon dioxide (CO_2), and volatile organic compounds (VOCs) play a vital role in maintaining a healthy indoor environment. These sensors provide real-time data that enables smart HVAC systems to adjust ventilation rates and air purification processes as needed. For example, if elevated levels of CO_2 are detected, the system can increase ventilation to dilute the indoor air, thus improving air quality and ensuring a healthier environment for occupants [46].

Table 7. Summary of Different IoT Sensors for Monitoring Indoor Air Quality Parameters and Their Applications in Building Management

Sensor Type	**IAQ Parameter Monitored**	**Application in Building Management**
Carbon Dioxide (CO_2)	CO_2 Concentration	Detects occupancy levels and ventilation needs, enabling dynamic control of HVAC systems to optimize energy use.
Particulate Matter (PM)	PM2.5, PM10 Levels	Monitors particulate concentrations to ensure air quality standards are met, crucial for occupant health.
Temperature Sensors	Indoor Temperature	Maintains thermal comfort by regulating heating and cooling systems based on real-time data.
Humidity Sensors	Relative Humidity	Controls moisture levels to prevent mold growth and maintain comfort; integrated with dehumidifiers.
Volatile Organic Compounds (VOC) Sensors	VOC Concentration	Detects harmful chemicals in the air, triggering ventilation or purification processes.
Carbon Monoxide (CO) Sensors	CO Levels	Ensures safety by detecting toxic CO levels and activating alarms or ventilation systems automatically.

Ozone (O_3) Sensors	Ozone Concentration	Monitors ozone levels to prevent exposure to high concentrations, important in urban buildings.
Nitrogen Dioxide (NO_2) Sensors	NO_2 Levels	Tracks nitrogen dioxide levels, which are critical for assessing traffic-related pollution indoors.

The table above provides a comprehensive summary of various IoT sensors used in monitoring key indoor air quality parameters within smart buildings. For instance, CO_2 sensors are crucial for detecting occupancy levels and optimizing ventilation to reduce energy consumption, as demonstrated by Taheri and Razban (2022) [47]. Similarly, Particulate Matter (PM) sensors help in maintaining air quality standards, a practice underscored by Johnson and Lee [48].

Temperature and humidity sensors are essential for ensuring occupant comfort and preventing issues like mold growth [49], [50]. Moreover, sensors for detecting Volatile Organic Compounds (VOCs) and Carbon Monoxide (CO) are vital for health and safety, triggering necessary actions when harmful concentrations are detected [51], [52].

Finally, Ozone (O_3) sensors and Nitrogen Dioxide (NO_2) sensors are particularly important in urban environments where pollution levels can significantly impact indoor air quality [53], [54].

2.8 Lighting Control

Lighting is another aspect of IEQ that significantly impacts both comfort and energy efficiency. IoT-enabled smart lighting systems use sensors to monitor natural light levels and occupancy patterns within a building. These systems can automatically adjust artificial lighting to complement natural light and respond to the presence of occupants. For example, in areas where natural light is abundant, smart lighting systems can dim or turn off lights to conserve energy while maintaining appropriate illumination levels. This approach not only contributes to energy savings but also enhances the visual comfort of building occupants [55].

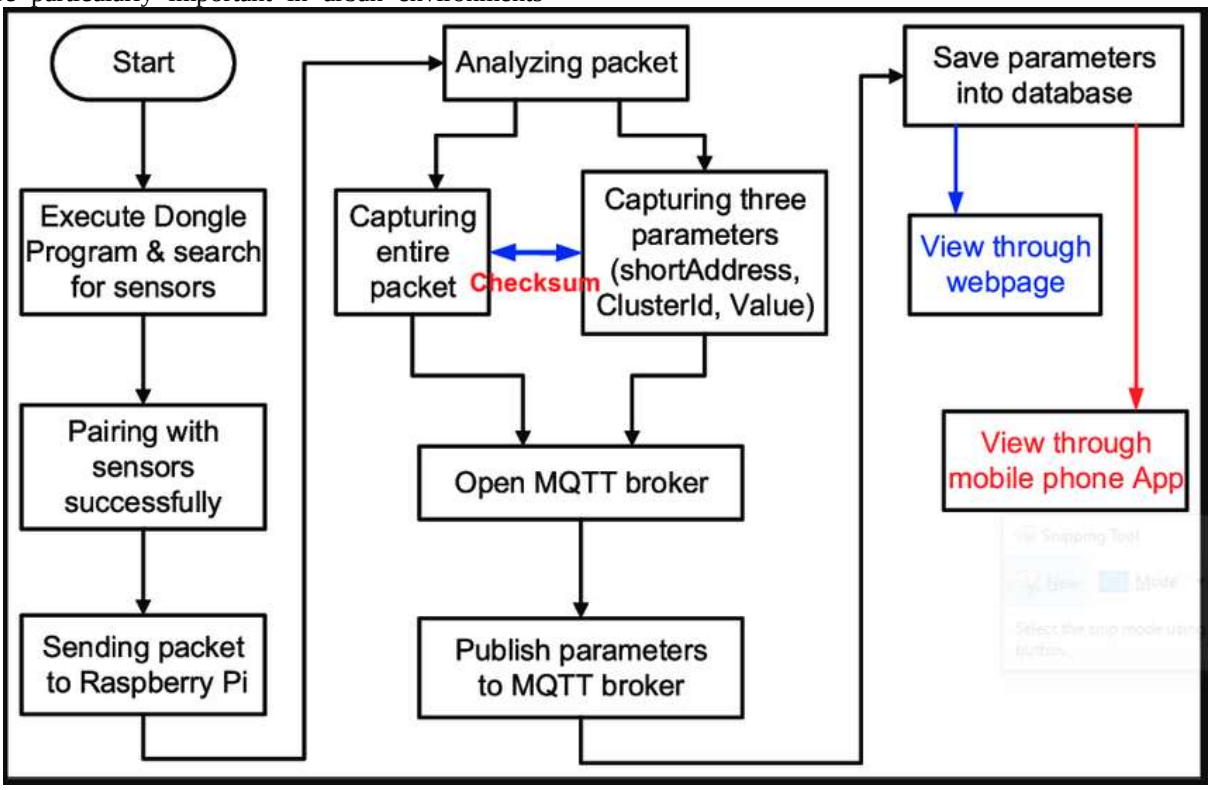


Figure 12. Flowchart showing the operation of an IoT-based smart lighting system, illustrating how sensors and control systems work together to optimize lighting levels based on natural light and occupancy [56].

2.8.1 Impact on Occupant Well-being

The ability to maintain optimal IEQ through IoT technologies has direct implications for occupant well-being. Studies have demonstrated that improved indoor environmental conditions are associated with increased productivity, reduced absenteeism, and overall better health outcomes for occupants

[57]. By continuously monitoring and adjusting environmental parameters, smart building systems ensure that occupants experience a comfortable and healthy indoor environment, which is crucial for both residential and commercial settings.

Table 8. Impact of Improved Indoor Environmental Quality on Occupant Well-Being [58].

IEQ Parameter	Metric	Impact on Occupant Well-Being
Air Quality	Reduced CO_2 Levels	Enhanced cognitive function and decision-making abilities, leading to increased productivity.
Thermal Comfort	Optimal Temperature Range (21-23°C)	Improved thermal satisfaction, reducing complaints and increasing overall comfort and focus.
Lighting Quality	Access to Natural Light and Adequate Illumination	Better visual comfort and mood enhancement, reducing eye strain and increasing work performance.
Acoustic Comfort	Low Noise Levels (< 45 dB)	Decreased stress levels and enhanced concentration, leading to better task performance.
Humidity Control	Maintaining 40-60% Relative Humidity	Lower incidence of respiratory issues and skin irritation, contributing to better health.
Ventilation Rate	8-12 Air Changes per Hour (ACH)	Reduced absenteeism due to fewer instances of sick building syndrome, enhancing overall productivity.
VOC Reduction	Low VOC Concentration	Decreased headaches and fatigue, resulting in improved well-being and productivity.

2.8.2 Space Utilization

Efficient space utilization is essential for maximizing the functionality and economic value of buildings, particularly in urban areas where space is at a premium. The integration of Internet of Things (IoT) technologies has transformed space management by providing real-time data on occupancy and usage patterns through devices such as occupancy sensors. This data, analyzed via advanced analytics platforms, reveals inefficiencies and trends that traditional methods might miss, enabling more effective space allocation and design [59]. By repurposing underutilized areas based on IoT insights, organizations can reduce costs and enhance productivity, particularly in commercial buildings where space is a significant cost factor. Furthermore, IoT data informs the strategic placement of physical assets, improving layout designs and promoting better circulation, safety, and collaboration in work environments [60].

IoT technologies also enhance user experiences by allowing for real-time adjustments to environmental factors like lighting and temperature, tailored to occupants' preferences. This personalization increases occupant satisfaction and the perceived value of the building, making it more attractive to tenants [61]. Additionally, IoT-driven strategies support sustainability by aligning space usage with actual demand, reducing energy consumption and the building's environmental footprint. For example, spaces with low usage can have reduced heating or lighting, further optimizing resource use [62].

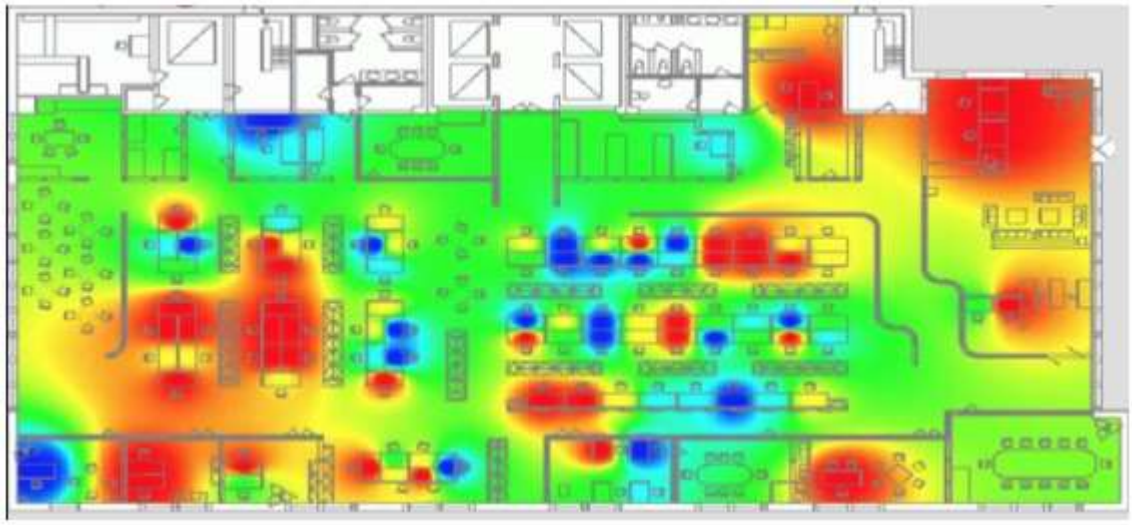


Figure 13. Heatmap showing space utilization patterns in a smart office building [63].

3. Challenges in IOT integration

3.1 Data Privacy and Security

One of the most significant challenges in the integration of IoT in smart buildings is ensuring data privacy and security. The vast amount of data collected by IoT devices poses risks related to unauthorized access, data breaches, and cyber-attacks. Protecting this data requires robust encryption, secure data storage, and regular security updates [64].

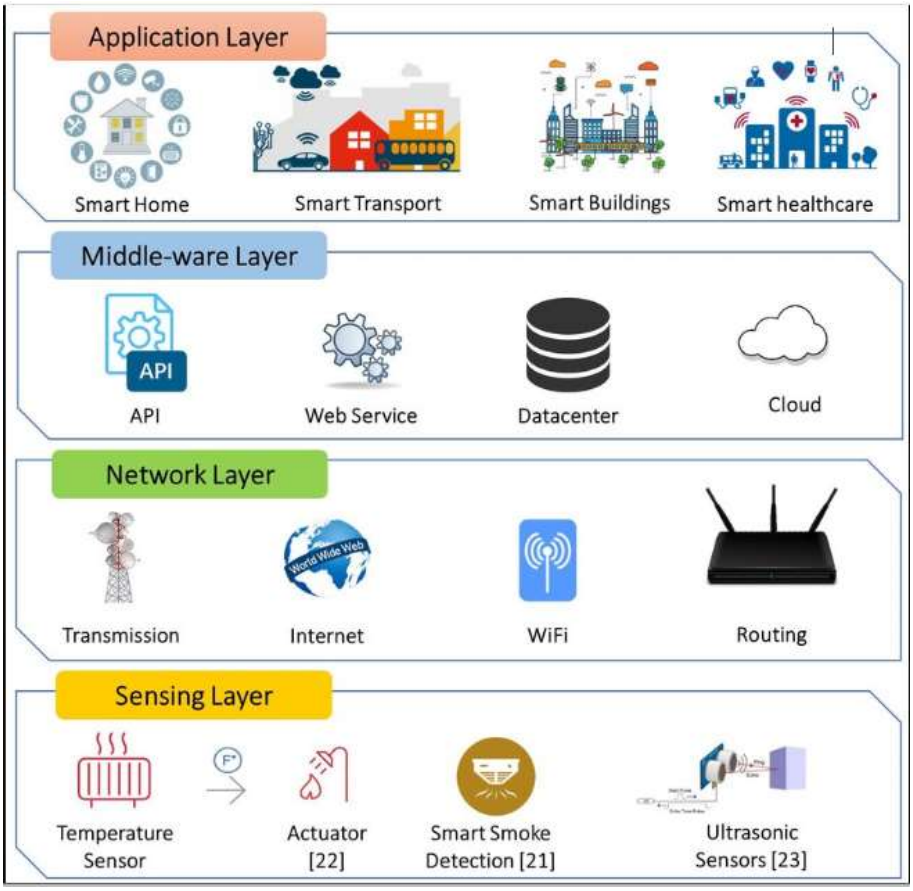


Figure 14. Diagram illustrating the layers of security in an IoT-based smart building system [65].

3.2 Interoperability

Interoperability is one of the most significant hurdles in the effective deployment of IoT technologies within smart buildings. As IoT systems grow more complex, the need for seamless communication between diverse devices, platforms, and protocols becomes increasingly important. However, the current landscape of IoT technologies is fragmented, with a lack of standardized protocols and communication methods, making it difficult to achieve full integration across various systems. This chapter delves into the interoperability challenges faced in the context of smart building IoT deployments, emphasizing the issues associated with multi-vendor ecosystems and the absence of universally accepted standards [66].

3.2.1 Fragmentation of IoT Devices and Standards

One of the primary challenges in IoT interoperability is the fragmentation of devices and standards. IoT ecosystems in smart buildings typically consist of a wide range of sensors, actuators, and communication systems that come from different manufacturers. These devices often use proprietary communication protocols, which limits their ability to interact with other devices or systems [67]. For instance, smart lighting systems from one manufacturer may not be able to communicate with HVAC controls from another, complicating the process of creating a fully integrated smart building.

Without common standards, device integration becomes a manual and labor-intensive process, often requiring custom-built middleware to facilitate communication between disparate systems. Moreover, the lack of standardization can create compatibility issues, preventing certain devices from working optimally or at all within a given ecosystem. These issues can lead to increased costs and inefficiencies, as building managers must either invest in specific, compatible technologies or retrofit existing systems to ensure operability [68].

3.2.2 Multi-Vendor Environments and Communication Barriers

In smart buildings, IoT devices often originate from multiple vendors, each with their own set of protocols and communication methods. This diversity leads to significant integration issues because devices from different manufacturers may not be designed to communicate effectively with one another [69]. For example, a smart security camera from one vendor may not be able to share data with a door lock system from another vendor without additional software layers to bridge the communication gap.

This lack of interoperability can hinder the general performance and efficiency of IoT systems in smart buildings. In multi-vendor environments, system integration typically requires the development of custom application programming interfaces (APIs) or middleware solutions to enable communication between devices. This increases both the complexity and cost of implementation, as building owners and managers need to hire specialized IT support to manage these integrations [70].

Furthermore, communication barriers between IoT devices can limit the ability to implement advanced features such as real-time data analysis or automated control. For example, if a smart thermostat cannot effectively communicate with occupancy sensors, the system may not be able to adjust temperature settings based on real-time occupancy data, reducing the potential energy savings and comfort improvements that IoT systems are designed to deliver [71].

3.2.3 The Lack of Universally Accepted Protocols

The absence of universally accepted protocols is another key factor contributing to the interoperability challenge. While some industry standards such as Zigbee, Z-Wave, and Bluetooth have been developed, these protocols are not always universally supported across devices, and their adoption varies by manufacturer [72]. As a result, smart buildings are often composed of devices that rely on different communication technologies, complicating efforts to integrate them into a unified system.

This lack of common communication standards can also create security vulnerabilities. Without standardized protocols, building managers may need to install multiple software patches or updates to ensure that different devices continue to function correctly. This opens up opportunities for cyber threats, as inconsistencies in protocol support can create loopholes in the system that attackers could exploit [73].

3.2.4. Potential Solutions and Future Directions

Efforts are underway to address the interoperability challenges in smart building IoT systems. Industry organizations are working on developing more comprehensive standards, such as the Internet Engineering Task Force's (IETF) Constrained Application Protocol (CoAP) and the Open Connectivity Foundation (OCF) standards, which aim to create a more uniform communication framework for IoT devices [74]. Additionally, cloud-based platforms are emerging as potential solutions to integration challenges. These platforms act as a central hub, aggregating data from various devices and systems, regardless of the communication protocol, to enable centralized control and data analysis.

However, despite these advancements, achieving seamless interoperability remains a complex and ongoing challenge. As IoT technology continues to evolve, it will be essential for manufacturers, developers, and standards bodies to work together to create more uniform frameworks that allow for the easy integration of devices from multiple vendors.

Table 9. Comparison of IoT Communication Protocols and Their Compatibility

Protocol	Frequency Band	Data Rate	Range	Power Consumption	Compatibility
Zigbee	2.4 GHz, 868 MHz, 915 MHz	250 kbps	10-100 meters	Low	Compatible with low-power, low-data rate devices; widely used in smart home and building automation systems
Wi-Fi (802.11n/ac/ax)	2.4 GHz, 5 GHz	Up to 9.6 Gbps (802.11ax)	50-100 meters (indoor)	High	High compatibility with most IoT devices; ideal for applications requiring high data rates, such as video surveillance
Bluetooth Low Energy (BLE)	2.4 GHz	125 kbps to 2 Mbps	10-100 meters	Very Low	Compatible with wearable devices and short-range communication; increasingly used in smart building sensors
LoRaWAN	Sub-GHz (433, 868, 915 MHz)	0.3-50 kbps	2-15 kilometers (urban)	Very Low	Compatible with wide-area networks; ideal for applications requiring long-range communication with low power consumption, such as environmental monitoring
NB-IoT	Licensed LTE bands	26 kbps to 250 kbps	10-15 kilometers	Low	High compatibility with cellular networks; suitable for applications needing reliable, long-range connectivity, such as smart metering
Z-Wave	908.42 MHz (US), 868.42 MHz (EU)	100 kbps	30-100 meters (indoor)	Low	Primarily used in home automation; compatible with a range of smart home devices, though limited by regional frequency allocations

Table 10. Cost-Benefit Analysis of IoT Implementation in Smart Buildings [75], [76]

Aspect	Costs	Benefits
Initial Investment	High upfront costs for IoT devices, sensors, and infrastructure setup	Long-term cost savings through energy efficiency, reduced maintenance costs, and operational efficiency
Installation and Integration	Costs associated with installing IoT systems and integrating with existing building management systems	Improved system interoperability, streamlined operations, and real-time data access that enhances decision-making
Maintenance and Upgrades	Ongoing costs for system maintenance, software updates, and hardware replacements	Predictive maintenance reduces unplanned downtime, extends equipment lifespan, and lowers overall maintenance costs
Data Management and Security	Expenses for data storage, processing, and cybersecurity measures	Enhanced data-driven decision-making, improved occupant safety, and compliance with data protection regulations
Training and Skill Development	Costs of training staff to operate and manage IoT systems	Increased staff proficiency, leading to better system management, faster response times, and higher overall efficiency
Energy Consumption	Potential increase in energy usage due to additional IoT devices	Significant reductions in energy consumption through optimized HVAC, lighting, and other building systems
Occupant Privacy Concerns	Costs related to ensuring compliance with privacy laws and addressing occupant concerns	Enhanced occupant trust and satisfaction, leading to higher occupancy rates and tenant retention

4. Future trends and research directions

4.1 Integration with AI and Machine Learning

The integration of AI and machine learning with IoT is expected to revolutionize smart buildings. AI can process the vast amounts of data generated by IoT devices, enabling advanced analytics, predictive modeling, and autonomous decision-making. For example, AI can be used to predict energy demand, optimize HVAC settings, or detect security threats before they occur [77].

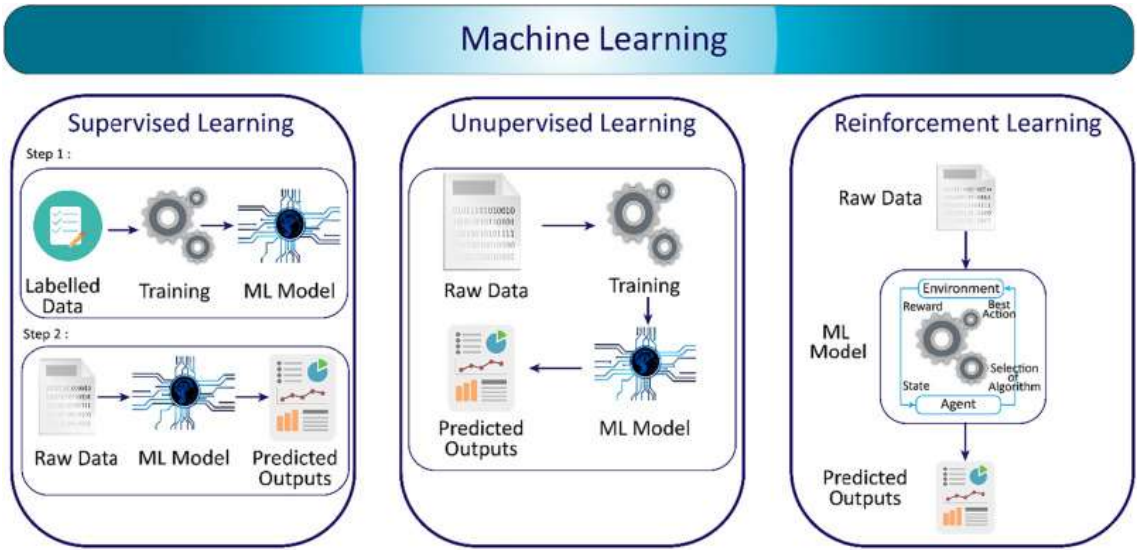


Figure 15. Interaction between AI, machine learning, and IoT in a smart building system [78].

4.2 Edge Computing

Edge computing is emerging as a critical technology for IoT in smart buildings. Unlike traditional cloud computing, which processes data in centralized data centers, edge computing processes data closer to the source. This approach reduces latency, improves real-time decision-making, and reduces the bandwidth required for data transmission [79].

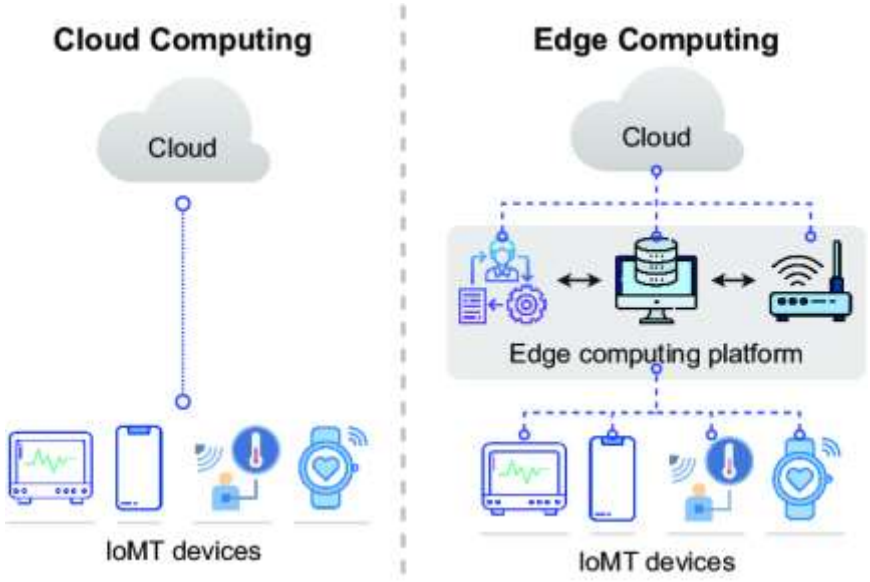


Figure 16. Diagram illustrating the difference between cloud computing and edge computing in IoT [80].

4.3 Sustainable Building Design

As sustainability becomes an increasingly important consideration in building design, the integration of IoT with sustainable building practices is likely to become more prevalent. IoT can provide real-time data on energy consumption, waste production, and water usage, enabling the optimization of these resources [81].

Table 11. Overview of IoT Applications in Sustainable Building Design [82], [83]

IoT Application	Function	Sustainability Impact

Smart HVAC Systems	Monitors and controls heating, ventilation, and air conditioning based on occupancy and environmental data	Reduces energy consumption and enhances indoor air quality by optimizing system performance
Automated Lighting Systems	Adjusts lighting levels according to natural light availability and occupancy	Lowers electricity usage and enhances occupant comfort through adaptive lighting solutions
Water Management Systems	Tracks and regulates water usage in real-time, including leak detection and irrigation control	Minimizes water waste and ensures efficient water use, contributing to water conservation efforts
Energy Monitoring and Management	Collects data on energy usage patterns and provides actionable insights for optimization	Enables real-time energy management, leading to significant reductions in carbon footprint
Waste Management Systems	Uses sensors to monitor waste levels and optimize collection schedules	Reduces the environmental impact of waste by improving efficiency in waste collection and disposal
Indoor Air Quality (IAQ) Monitoring	Continuously monitors CO_2 levels, humidity, and VOCs, adjusting ventilation as needed	Enhances occupant health and productivity by maintaining optimal air quality while reducing energy usage
Smart Metering Systems	Provides detailed insights into individual energy and water consumption for each tenant	Encourages responsible resource use and supports tenant participation in sustainability initiatives

5. Conclusion

The security of IoT systems is particularly important in the context of smart buildings, where an increasing number of connected devices collect, share, and process sensitive data. Cybersecurity threats are a significant concern, and the protection of this data is essential for maintaining user trust and safeguarding operations. The reliability of IoT systems is equally vital, especially in environments where continuous operation is critical, such as hospitals, corporate offices, or large-scale residential complexes. Any disruptions could lead to operational inefficiencies or compromised safety. Additionally, the scalability of IoT solutions ensures that these technologies can grow and evolve with the buildings they support, adapting to new demands without a loss in performance or capability.

Looking towards the future, the full potential of IoT in the built environment will only be realized through the creation of intelligent systems that can dynamically respond to the changing needs of occupants. These systems will enhance not only comfort but also safety, energy use, and overall building efficiency. As cities become more densely populated and resources more strained, IoT-driven smart buildings will be critical in advancing global sustainability efforts. Through the integration of energy-efficient technologies, predictive maintenance tools, and smart resource management systems, IoT can help mitigate environmental impact while creating buildings that are more adaptive and responsive to their users.

However, realizing this future requires continued investment in research and development. The field of IoT is rapidly evolving, and advancements in areas such as artificial intelligence, machine learning, and data analytics will be essential for overcoming existing limitations. Issues such as interoperability, data privacy, and system integration remain significant hurdles that must be addressed to achieve widespread adoption and optimal performance of IoT solutions in the built environment. Therefore, ongoing research is critical to refining these technologies and ensuring that the promise of smart buildings is fully realized.

Hence, while IoT technologies offer tremendous opportunities for revolutionizing the built environment, their success depends on careful consideration of security, reliability, and scalability. The future of smart buildings lies in harnessing IoT's potential to create intelligent, responsive environments that align with both the evolving needs of occupants and the broader goal of sustainability. Continued innovation and research will be key to overcoming current challenges and unlocking the full capabilities of IoT in shaping the future of the built environment.

References

1. Verma, A., Prakash, S., Srivastava, V., Kumar, A., & Mukhopadhyay, S. (2019). Sensing, Controlling, and IoT Infrastructure in Smart Building: A Review. *IEEE Sensors Journal*, 19, 9036-9046. https://doi.org/10.1109/JSEN.2019.2922409.

2. Esrafilian-Najafabadi, M., & Haghighat, F. (2021). Occupancy-based HVAC control systems in buildings: A state-of-the-art review. *Building and Environment*. https://doi.org/10.1016/J.BUILDENV.2021.107810.

3. Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. (2020). Internet of Things (IoT) and the Energy Sector. *Energies*. https://doi.org/10.3390/en13020494.

4. Xu, X., Lin, M., Chen, K., & Yao, Z. (2023). An Environmental and Security Monitoring System Based on IoT. *2023 IEEE 3rd International Conference on Electronic Technology, Communication and Information (ICETCI)*, 1354-1361. https://doi.org/10.1109/ICETCI57876.2023.10176803.

5. Alkhudaydi, O., Krichen, M., & Alghamdi, A. (2023). A Deep Learning Methodology for Predicting Cybersecurity Attacks on the Internet of Things. *Information*. https://doi.org/10.3390/info14100550.

6. Tariq, U., Ahmed, I., Bashir, A., & Shaukat, K. (2023). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors (Basel, Switzerland)*, 23. https://doi.org/10.3390/s23084117.

7. Balti, M., Somrani, G., Jemai, A., & Bouhachem, M. (2023). AI Based Video and Image Analytics. *2023 International Conference on Innovations in Intelligent Systems and Applications (INISTA)*, 1-6. https://doi.org/10.1109/INISTA59065.2023.10310403.

8. Saini, M., Aggarwal, A., & Saini, S. (2020). Challenges in the Area of IoT., 87-105. https://doi.org/10.4018/978-1-5225-9574-8.ch004.

9. Luo, J. (2022). A Bibliometric Review on Artificial Intelligence for Smart Buildings. *Sustainability*. https://doi.org/10.3390/su141610230.

10. Markets and market (2024). Intelligent Building Automation Technologies Market. https://www.marketsandmarkets.com/Market-Reports/building-technology-346.html)

11. Aliero, M., Asif, M., Ghani, I., Pasha, M., & Jeong, S. (2022). Systematic Review Analysis on Smart Building: Challenges and Opportunities. *Sustainability*. https://doi.org/10.3390/su14053009.

12. Stanelytė, D., Radziukynienė, N., & Radziukynas, V. (2022). Overview of Demand-Response Services: A Review. *Energies*. https://doi.org/10.3390/en15051659.

13. Kee, K. K., Shahab, S. M. F., & Loh, C. J. (2016). *Design and development of an innovative smart metering system with GUI-based NTL detection platform. 4th IET Clean Energy and Technology Conference (CEAT 2016).* doi:10.1049/cp.2016.1293

14. Plando, J. (2023). Advancements in Smart Thermostat Technology for Enhanced HVAC Energy Management. *International Journal of Advanced Research in Science, Communication and Technology*. https://doi.org/10.48175/ijarsct-12388.

15. Ahmad, K., Rafique, A. F., & Badshah, S. (2014). Energy Efficient Residential Buildings in Pakistan. Energy & Environment, 25(5), 991-1002. https://doi.org/10.1260/0958-305X.25.5.991)

16. Kim, D., Lee, J., Do, S., Mago, P., Lee, K., & Cho, H. (2022). Energy Modeling and Model Predictive Control for HVAC in Buildings: A Review of Current Research Trends. *Energies*. https://doi.org/10.3390/en15197231.

17. Merabet, G., Essaaidi, M., Haddou, M., Qolomany, B., Qadir, J., Anan, M., Al-Fuqaha, A., Abid, M., & Benhaddou, D. (2021). Intelligent Building Control Systems for Thermal Comfort and Energy-Efficiency: A Systematic Review of Artificial Intelligence-Assisted Techniques. *ArXiv*, abs/2104.02214. https://doi.org/10.1016/J.RSER.2021.110969.

18. Al-Obaidi, K., Hossain, M., Alduais, N., Al-Duais, H., Omrany, H., & Ghaffarianhoseini, A. (2022). A Review of Using IoT for Energy Efficient Buildings and Cities: A Built Environment Perspective. *Energies*. https://doi.org/10.3390/en15165991.

19. Mahmoud, M. (2021) Automated Smart Utilization of Background Lights and Daylight for Green Building Efficient and Economic Indoor Lighting Intensity Control. *Intelligent Control and Automation*, **12**, 1-15. doi: 10.4236/ica.2021.121001.

20. Mishra, P., & Singh, G. (2023). Energy Management Systems in Sustainable Smart Cities Based on the Internet of Energy: A Technical Review. *Energies*. https://doi.org/10.3390/en16196903.

21. Naik, P., & Kunte, R. (2023). Review of Literature on Human Activity Detection and Recognition. *International Journal of Management, Technology, and Social Sciences*. https://doi.org/10.47992/ijmts.2581.6012.0318.

22. Netinant, Paniti, Thitipong Utsanok, Meennapa Rukhiran, and Suttipong Klongdee. 2024. "Development and Assessment of Internet of

Things-Driven Smart Home Security and Automation with Voice Commands" *IoT* 5, no. 1: 79-99. https://doi.org/10.3390/iot5010005

23. D, B., & Cg, A. (2023). Securexa: A Facial Recognition-Based Security System – Review of Literature, Research Analysis & Methodology. *International Scientific Journal of Engineering and Management*. https://doi.org/10.55041/isjem00358.

24. Rehman, A. ur, Rehman, S. ur, Khan, I. U., Moiz, M., & Hasan, S. (2022). Security and Privacy Issues in IoT. *International Journal of Communication Networks and Information Security (IJCNIS)*, *8*(3). https://doi.org/10.17762/ijcnis.v8i3.2074

25. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L., & Abdulkadir, S. (2022). Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review. *Electronics*. https://doi.org/10.3390/electronics11020198.

26. Nazir, Anjum, Zulfiqar Memon, Touseef Sadiq, Hameedur Rahman, and Inam Ullah Khan. 2023. "A Novel Feature-Selection Algorithm in IoT Networks for Intrusion Detection" *Sensors* 23, no. 19: 8153. https://doi.org/10.3390/s23198153

27. Borisova, A., & Nikolov, L. (2023). Systems with Artificial Intelligence for Defense and Security. *Scientific Research and Education in the Air Force*. https://doi.org/10.19062/2247-3173.2023.24.7.

28. Nassif, A., Talib, M., Nasir, Q., & Dakalbab, F. (2021). Machine Learning for Anomaly Detection: A Systematic Review. *IEEE Access*, 9, 78658-78700. https://doi.org/10.1109/ACCESS.2021.3083060.

29. Cinar, Eyup, Sena Kalay, and Inci Saricicek. 2022. "A Predictive Maintenance System Design and Implementation for Intelligent Manufacturing" *Machines* 10, no. 11: 1006. https://doi.org/10.3390/machines10111006

30. Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K., & O'Neill, Z. (2022). A critical review of cyber-physical security for building automation systems. *Annu. Rev. Control.*, 55, 237-254. https://doi.org/10.1016/j.arcontrol.2023.02.004.

31. Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2021). A review of video surveillance systems. *J. Vis. Commun. Image Represent.*, 77, 103116. https://doi.org/10.1016/J.JVCIR.2021.103116.

32. Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H., & Djukic, P. (2022). Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats. *ACM Computing Surveys*, 55, 1 - 37. https://doi.org/10.1145/3530812.

33. Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access*, 8, 153826-153848. https://doi.org/10.1109/ACCESS.2020.3018170.

34. Stolojescu-Crisan, Cristina, Calin Crisan, and Bogdan-Petru Butunoi. 2021. "An IoT-Based Smart Home Automation System" *Sensors* 21, no. 11: 3784. https://doi.org/10.3390/s21113784

35. Kotenko, I., Izrailov, K., & Buinevich, M. (2022). Static Analysis of Information Systems for IoT Cyber Security: A Survey of Machine Learning Approaches. *Sensors (Basel, Switzerland)*, 22. https://doi.org/10.3390/s22041335.

36. Liao, B., Ali, Y., Nazir, S., He, L., & Khan, H. (2020). Security Analysis of IoT Devices by Using Mobile Computing: A Systematic Literature Review. *IEEE Access*, 8, 120331-120350. https://doi.org/10.1109/ACCESS.2020.3006358.

37. Singh, R., Kukreja, D., & Sharma, D. (2023). Blockchain-enabled access control to prevent cyber-attacks in IoT: Systematic literature review. *Frontiers in Big Data*, 5. https://doi.org/10.3389/fdata.2022.1081770.

38. Pittaras, I., & Polyzos, G. (2023). Multi-tenant, Decentralized Access Control for the Internet of Things. *2023 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)*, 28-34. https://doi.org/10.1109/IoTaIS60147.2023.10346081.

39. Soltani, N., Rahmani, A., Bohlouli, M., & Hosseinzadeh, M. (2022). Artificial intelligence empowered threat detection in the Internet of Things: A systematic review. *Concurrency and Computation: Practice and Experience*, 34. https://doi.org/10.1002/cpe.6894.

40. Abbas, A., Khan, M.A., Latif, S. (2022). A New Ensemble-Based Intrusion Detection System for

Internet of Things. *Arab J Sci Eng* 47, 1805–1819. https://doi.org/10.1007/s13369-021-06086-5

41. Broday, E., & Silva, M. (2022). The role of internet of things (IoT) in the assessment and communication of indoor environmental quality (IEQ) in buildings: a review. *Smart and Sustainable Built Environment*. https://doi.org/10.1108/sasbe-10-2021-0185.

42. Carli, R., Cavone, G., Othman, S., & Dotoli, M. (2020). IoT Based Architecture for Model Predictive Control of HVAC Systems in Smart Buildings. *Sensors (Basel, Switzerland)*, 20. https://doi.org/10.3390/s20030781.

43. Sahoh, Bukhoree, Mallika Kliangkhlao, and Nichnan Kittiphattanabawon. (2022). "Design and Development of Internet of Things-Driven Fault Detection of Indoor Thermal Comfort: HVAC System Problems Case Study" *Sensors* 22, no. 5: 1925. https://doi.org/10.3390/s22051925

44. Marzouk, M., & Atef, M. (2022). Assessment of Indoor Air Quality in Academic Buildings Using IoT and Deep Learning. *Sustainability*. https://doi.org/10.3390/su14127015.

45. Floris, A., Porcu, S., Girau, R., & Atzori, L. (2021). An IoT-Based Smart Building Solution for Indoor Environment Management and Occupants Prediction. *Energies*, 14, 2959. https://doi.org/10.3390/EN14102959.

46. Wu, H., & Wong, J. (2022). Temperature versus Relative Humidity: Which Is More Important for Indoor Mold Prevention? *Journal of Fungi*, 8. https://doi.org/10.3390/jof8070696.

47. Taheri, S., & Razban, A. (2021). Learning-based CO2 concentration prediction: Application to indoor air quality control using demand-controlled ventilation. *Building and Environment*, 205, 108164. https://doi.org/10.1016/J.BUILDENV.2021.108164.

48. Kuncoro, C., Permana, A., Asyikin, M., & Adristi, C. (2022). Smart Wireless Climate Sensor Node for Indoor Comfort Quality Monitoring Application. *Energies*. https://doi.org/10.3390/en15082939.

49. Khatib, M., & Haick, H. (2022). Sensors for Volatile Organic Compounds. *ACS nano*. https://doi.org/10.1021/acsnano.1c10827.

50. Mohammadzadeh, M., Hasani, A., Jaferzadeh, K., Fawzy, M., Silva, T., Abnavi, A., Ahmadi, R., Ghanbari, H., Askar, A., Kabir, F., Rajapakse, R., & Adachi, M. (2023). Unique Photoactivated Time-Resolved Response in 2D GeS for Selective Detection of Volatile Organic Compounds. *Advanced Science*, 10. https://doi.org/10.1002/advs.202205458.

51. Hasan, M., Yu, H., Ivey, C., Pillarisetti, A., Yuan, Z., Do, K., & Li, Y. (2023). Unexpected Performance Improvements of Nitrogen Dioxide and Ozone Sensors by Including Carbon Monoxide Sensor Signal. *ACS Omega*, 8, 5917 - 5924. https://doi.org/10.1021/acsomega.2c07734.

52. Baldelli, A. (2021). Evaluation of a low-cost multi-channel monitor for indoor air quality through a novel, low-cost, and reproducible platform. , 17, 100059. https://doi.org/10.1016/J.MEASEN.2021.100059.

53. Tanasiev, V., Necula, H., Alistar, A., Patru, G., & Badea, A. (2021). Energy-Efficient Solution for Smart Lighting Through IoT. *2021 10th International Conference on ENERGY and ENVIRONMENT (CIEM)*, 1-4. https://doi.org/10.1109/ciem52821.2021.9614714.

54. JUNE THARAPHE LWIN1, AUNG ZE YA 2. (2015). Development of Microcontroller Based Temperature and Lighting Control System in Smart Home. International Journal of Scientific Engineering and Technology Research. ISSN 2319-8885 Vol.03, Issue.16 July-2014, Pages:3322-3327. Volume.03, IssueNo.16, July-2014, Pages: 3322-3327

55. Broday, E., & Silva, M. (2022). The role of internet of things (IoT) in the assessment and communication of indoor environmental quality (IEQ) in buildings: a review. *Smart and Sustainable Built Environment*. https://doi.org/10.1108/sasbe-10-2021-0185.

56. Sung, G.-M., Shen, Y.-S., Hsieh, J.-H., & Chiu, Y.-K. (2019). *Internet of Things–based smart home system using a virtualized cloud server and mobile phone app. International Journal of Distributed Sensor Networks, 15(9), 155014771987935.* doi:10.1177/1550147719879354

57. Azizi, S., Nair, G., Rabiee, R., & Olofsson, T. (2020). Application of Internet of Things in academic buildings for space use efficiency using occupancy and booking data. *Building and Environment*, 186, 107355 - 107355. https://doi.org/10.1016/j.buildenv.2020.107355.

58. Foster, G. (2020). Circular economy strategies for adaptive reuse of cultural heritage buildings to reduce environmental impacts. *Resources, Conservation and Recycling*. https://doi.org/10.1016/j.resconrec.2019.104507.

59. Hajjaji, Y., Boulila, W., Farah, I., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. *Comput. Sci. Rev.*, 39, 100318. https://doi.org/10.1016/j.cosrev.2020.100318.

60. Hafeez, G., Wadud, Z., Khan, I., Khan, I., Shafiq, Z., Usman, M., & Khan, M. (2020). Efficient Energy Management of IoT-Enabled Smart Homes Under Price-Based Demand Response Program in Smart Grid. *Sensors (Basel, Switzerland)*, 20. https://doi.org/10.3390/s20113155.

61. Sameera Ghayyur, Xi He, Dhrubajyoti Ghosh, Sharad Mehrotra (2019). Towards Accuracy Aware Minimally Invasive Monitoring (MiM) Conference: ACM Conference on Computer and Communications Security (Theory and Practice of Differential Privacy https://www.researchgate.net/publication/339080862_Towards_Accuracy_Aware_Minimally_Invasive_Monitoring_MiM.

62. Inibhunu, C., & McGregor, C. (2021). Privacy Preserving Framework for Big Data Management in Smart Buildings. *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 667-673. https://doi.org/10.1109/PerComWorkshops51409.2021.9430994.

63. Wu, CK. (2021). IoT Security Architecture. In: Internet of Things Security. Advances in Computer Science and Technology. Springer, Singapore. https://doi.org/10.1007/978-981-16-1372-2_3

64. Farooq, M., Wheelock, I., & Pesch, D. (2020). IoT-Connect: An Interoperability Framework for Smart Home Communication Protocols. *IEEE Consumer Electronics Magazine*, 9, 22-29. https://doi.org/10.1109/MCE.2019.2941393.

65. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). *A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 1–1.* doi:10.1109/access.2019.2924045

66. Farooq, M., Wheelock, I., & Pesch, D. (2020). IoT-Connect: An Interoperability Framework for Smart Home Communication Protocols. *IEEE Consumer Electronics Magazine*, 9, 22-29. https://doi.org/10.1109/MCE.2019.2941393.

67. Simeoni, E., Gaeta, E., García-Betances, R., Raggett, D., Gil, A., Carvajal-Flores, D., Fico, G., Cabrera-Umpiérrez, M., & Arredondo, M. (2021). A Secure and Scalable Smart Home Gateway to Bridge Technology Fragmentation. *Sensors (Basel, Switzerland)*, 21. https://doi.org/10.3390/s21113587.

68. Gandal, N. (2002). Compatibility, Standardization, and Network Effects: Some Policy Implications. *Oxford Review of Economic Policy*, 18, 80-91. https://doi.org/10.1093/OXREP/18.1.80.

69. Al-Obaidi, K., Hossain, M., Alduais, N., Al-Duais, H., Omrany, H., & Ghaffarianhoseini, A. (2022). A Review of Using IoT for Energy Efficient Buildings and Cities: A Built Environment Perspective. *Energies*. https://doi.org/10.3390/en15165991.

70. Mosterman, P., & Zander, J. (2016). Cyber-physical systems challenges: a needs analysis for collaborating embedded software systems. *Software & Systems Modeling*, 15, 5-16. https://doi.org/10.1007/s10270-015-0469-x.

71. Wang, C., Pattawi, K., & Lee, H. (2020). Energy saving impact of occupancy-driven thermostat for residential buildings. *Energy and Buildings*, 211, 109791. https://doi.org/10.1016/j.enbuild.2020.109791.

72. Wang, W., Liu, X., Yao, Y., & Zhu, T. (2023). Simultaneous Data Dissemination Among WiFi and ZigBee Devices. *IEEE/ACM Transactions on Networking*, 31, 2545-2558. https://doi.org/10.1109/TNET.2023.3243070.

73. Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K., & O'Neill, Z. (2022). A critical review of cyber-physical security for building automation systems. *Annu. Rev. Control.*, 55, 237-254. https://doi.org/10.1016/j.arcontrol.2023.02.004.

74. Sinche, S., Raposo, D., Armando, N., Rodrigues, A., Boavida, F., Pereira, V., & Silva, J. (2020). A Survey of IoT Management Protocols and Frameworks. *IEEE Communications Surveys & Tutorials*, 22, 1168-1190. https://doi.org/10.1109/COMST.2019.2943087.

75. Shanaka Kristombu Baduge, Sadeep Thilakarathna, Jude Shalitha Perera, Mehrdad Arashpour, Pejman Sharafi, Bertrand Teodosio, Ankit Shringi, Priyan Mendis, (2022).Artificial intelligence and smart vision for building and construction 4.0: Machine

and deep learning methods and applications, Automation in Construction,Volume 141,104440,ISSN 0926-5805, https://doi.org/10.1016/j.autcon.2022.104440.

76. Chen, B., Wan, J., Celesti, A., Li, D., Abbas, H., & Zhang, Q. (2018). Edge Computing in IoT-Based Manufacturing. *IEEE Communications Magazine*, 56, 103-109. https://doi.org/10.1109/MCOM.2018.1701231.

77. Chengoden, R., Victor, N., Huynh-The, T., Yenduri, G., Jhaveri, R., Alazab, M., Bhattacharya, S., Hegde, P., Maddikunta, P., & Gadekallu, T. (2022). Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions. *IEEE Access*, 11, 12764-12794. https://doi.org/10.1109/ACCESS.2023.3241628.

78. Krishnan, P., Prabu, A., Loganathan, S., Routray, S., Ghosh, U., & Al-Numay, M. (2023). Analyzing and Managing Various Energy-Related Environmental Factors for Providing Personalized IoT Services for Smart Buildings in Smart Environment. *Sustainability*. https://doi.org/10.3390/su15086548.

79. Xu, X., Liu, X., Xu, Z., Dai, F., Zhang, X., & Qi, L. (2020). Trust-Oriented IoT Service Placement for Smart Cities in Edge Computing. *IEEE Internet of Things Journal*, 7, 4084-4091. https://doi.org/10.1109/JIOT.2019.2959124.

80. Chengoden, Rajeswari & Victor, Nancy & Huynh-The, Thien & Yenduri, Gokul & Jhaveri, Rutvij & Alazab, Mamoun & Bhattacharya, Sweta & Hegde, Pawan & Maddikunta, Praveen & Gadekallu, Thippa. (2023). Metaverse for Healthcare: A Survey on Potential Applications, Challenges and Future Directions. IEEE Access. PP. 1-1. 10.1109/ACCESS.2023.3241628.

81. Iwendi, C., Maddikunta, P., Gadekallu, T., Lakshmanna, K., Bashir, A., & Piran, M. (2020). A metaheuristic optimization approach for energy efficiency in the IoT networks. *Software: Practice and Experience*, 51, 2558 - 2571. https://doi.org/10.1002/spe.2797.

82. Taha, A., & Elabd, A. (2021). IoT for Certified Sustainability in Smart Buildings. *IEEE Network*, 35, 241-247. https://doi.org/10.1109/mnet.011.2000521.

83. Chen, Y., Wang, X., Liu, Z., Cui, J., Osmani, M., & Demian, P. (2023). Exploring Building Information Modeling (BIM) and Internet of Things (IoT) Integration for Sustainable Building. *Buildings*. https://doi.org/10.3390/buildings13020288.